Kazenas German Vladimirovich
Student
Ural Federal University
Russia, Ekaterinburg
Academic supervisor: Kovaleva Alexandra Georgievna

APPLICATION OF WIRESHARK FOR DETECTING INFORMATION SECURITY INCIDENTS

Abstract. *Wireshark is a widely used traffic and packet analyzer. This article is devoted to practical methods of detecting information security incidents in an enterprise network based on traffic analysis using the Wireshark packet analyzer. Attacks such as ARP-spoofing, DDoS are considered, detection of the presence of bots in the network is regarded both by direct and indirect characteristics, and the main points of detection of connection to the Tor network are presented.*

Keywords: *Wireshark, digital forensics, packet analysis, information security.*

Казенас Герман Владимирович
Студент
Уральский федеральный университет
Россия, г. Екатеринбург
Научный руководитель: Ковалева Александра Георгиевна

ПРИМЕНЕНИЕ WIRESHARK ДЛЯ ДЕТЕКТРИОВАНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: *Wireshark является широко используемым анализатором сетевых протоколов и пакетов. Данная статья посвящена практическим способам детектирования инцидентов информационной безопасности в сети предприятия на основе анализа трафика с помощью анализатора пакетов*

Wireshark. Рассмотрены такие атаки как ARP-spoofing, DDoS, рассмотрено детектирование наличия ботов в сети как по прямым признакам, так и по косвенным, представлены основные пункты детектирования подключения к сети Tor.

Ключевые слова: *Wireshark, цифровая криминалистика, анализ пакетов, информационная безопасность.*

The modern world is unthinkable without computers. A man has reached out to the whole world with information networks. An infinite amount of information circulates between computers. The lives of people, companies, corporations, and governments depend on them. Networks are «roads» where anyone can get information. But the legitimacy of getting information remains to be seen.

In 2019, more than 2.5 trillion rubles were lost [1]. But according to statistics from the Russian Prosecutor General's Office only a quarter of crimes are solved. That is, most of the money is not returned. Business is in danger! There is a solution. This is the investigation of crimes and digital forensics. It is important to respond to an information security incident as early as possible. The paper discusses the use of Wireshark for detecting and responding to information security incidents in an enterprise network.

The above advantages of this packet analyzer [3] make it possible to detect several popular and dangerous attacks on a network. The first variant of attack considered may be ARP spoofing. This type of attack refers to attacks like MITM («Man In The Middle»).

ARP protocol is designed to translate IP addresses into MAC addresses. Most often it is a conversion to Ethernet addresses, but ARP is also used in networks of other technologies: Token Ring, FDDI and others. But Wireshark may also work with these networks, which is undoubtedly another advantage of this program. The ARP protocol is absolutely unprotected. It does not have any means of verifying the authenticity of packets: both requests and responses. There are records with each other's IP and MAC addresses in the ARP table of nodes A and B before performing ARP-spoofing. The

information is exchanged directly between nodes A and B. During the ARP-spoofing process, computer C executing the attack sends ARP replies:

- to Node A: with the IP address of Node B and the MAC address of Node C;
- Node B: with the IP address of node A and the MAC address of node C.

Due to the fact that computers support spontaneous ARP (gratuitous ARP), they modify their own ARP tables and place entries where the real MAC addresses of computers A and B are replaced by the MAC address of the computer C.

Wireshark clearly reflects the presence of an attack in the past, as well as the direct course of the attack. The Figure 1 demonstrates the overall case of an ARP packet, and the MAC addresses of the sender and the recipient. Since ARP spoofing involves spoofing the MAC address, it is possible to monitor these addresses in real time and sound an alarm if they change.

Duplicate files appear with this type of attacks. They may also be detected with Wireshark by entering the keyword arp.duplicate-addressdetected [4] in the filter (Figure 1).

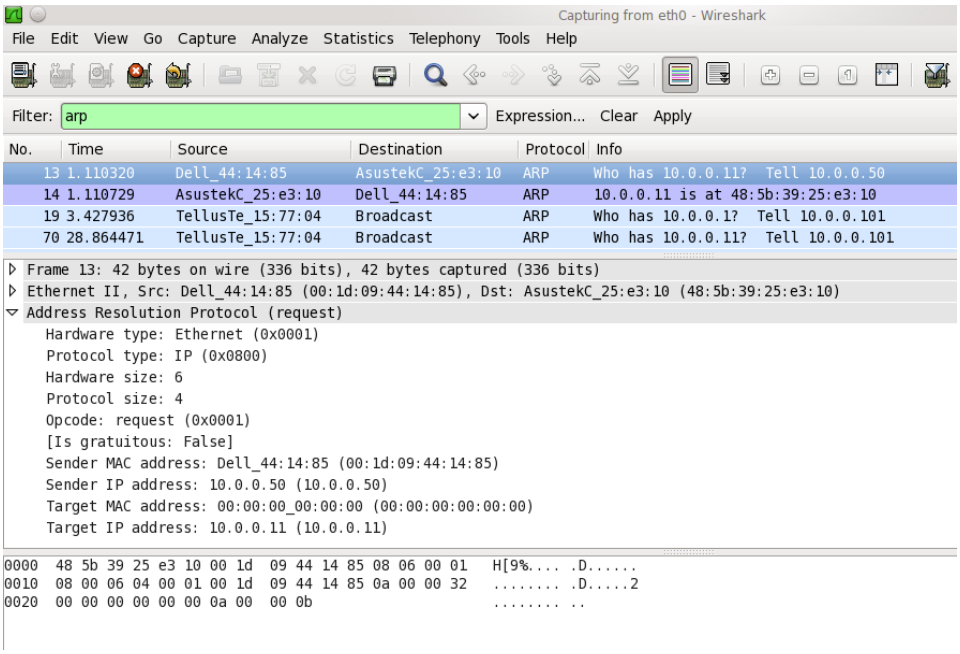

Figure 1 – Typical ARP packet

Another very common type of attack is the denial of service attack (DoS or DDoS). DoS or «denial of service» is an attack on a computer system in order to bring it to failure, i.e. to create conditions under which system users will not be able to access

the provided resources, or this access will be difficult. The distributed denial of service attack - or DDoS (Distributed Denial of Service) - is a simultaneous and massive sending of information requests to a central server. An attacker generates such requests using a large number of compromised systems. These compromised systems may be botnets. A botnet network is a network of a large number of distributed devices that are managed programmatically. These devices have access to the network and can generate huge amounts of traffic directed to the target system [5].

DDoS attacks may be conducted at different layers of the OSI model, using different protocols. But thanks to Wireshark, which works with protocols of different layers, their detection may be minimized by using packet analyzers [2]. But a large amount of traffic puts a lot of load on the system, which can disable it. A quick and accurate solution is therefore needed to detect such attacks. Machine learning does not stand still and now the combination of machine learning and information security is a trend [9]. One of the main entry points for machine learning into network security is packet analysis. These algorithms first remember the simple network usage pattern and then the attack pattern (training with the teacher) [6, 7].

Also, deep packet analysis programs may work with different levels of attack. But these algorithms cannot work without a packet analyzer. This is Wireshark. That algorithms may be configured when teaching systems with its help, because sometimes it is impossible to distinguish artificial attack traffic from simple network usage by many users [8].

Detecting botnets is not the most trivial task. A couple of packets cannot be determined exactly whether the traffic is malicious or not. Regular botnets and IoT botnets should also be distinguished. The difference is that the Internet devices of things in normal uninfected state cannot generate some types of packets. This makes it easy to detect them in terms of packet analysis.

Special systems such as BotMiner, BoNeSSy and others have been created to detect botnets. They use various sophisticated algorithms to detect malicious botnet traffic, where clustering is the main one [9]. Different botnets also use different types of management traffic, such as IPC, HTTP, HTTPS, P2P. And the detection of

malicious packets cannot be done manually. Many systems use Wireshark during the design phase to better manage the training process and to correct systems, and only then, when the system is introduced into the testing phase, they leave only the library of packet captures.

In the investigation of incidents, sometimes a method of incident detection is used, it is not prevented, but used in order to collect more information about the incident. One such incident is the Tor network access. Tor is a system of proxy servers that allows establishing an anonymous network connection that is protected from eavesdropping. Tor is seen as an anonymous network of virtual tunnels, providing data transmission in encrypted form. Many hackers use Tor to hide their data on the network. They can also be used for remote management from a remote command line or a remote desktop. In this scenario it is impossible to distinguish between Tor network traffic and ordinary HTTPS traffic when a connection is established. Some unscrupulous employees may use the Tor network for illegal activities, such as buying drugs, leaks of confidential information.

Complete anonymity and protection cannot be guaranteed even on the Tor network without certain rules of behavior. There are many malefactors in this network who can use this data for gain. But fortunately, you can track the certificate when you connect to a Tor network node, thus determining if you are connected to the network. Further actions on the investigation are taken by specialists [10].

Many security professionals also explore alternative ways of organizing their network for a security perspective. One such type of network building is peer-to-peer network. A peer-to-peer network is a computer network based on equality of participants. Often, in such a network there are no dedicated servers, each node is both client and server. In contrast to the client-server architecture, such an organization allows keeping the network running at any number and any combination of available nodes. Peer-to-peer (P2P) networks may be used both for legal traffic exchange, such as torrents, and for criminal activities, including botnet management. But communication between the nodes in such a network can be easily traced using a traffic analyzer. When listening to traffic, it may turn out that several clients are trying to

access information on the server. Thus, it is possible to determine the IP addresses that participate in this peering network [11].

After all, it is logically impossible not to mention the heart of Wireshark. The traffic capturing library, which is used in Wireshark, is also very popular. It is used not only in network traffic displaying tools, but also in port scanning utilities and network attack detection systems. Due to its versatility, this library has acquired many wrappers for use in other programming languages. On its basis, separate libraries for traffic capture, such as Scapy [12], are written. It is important to be able to select the necessary tools, rather than dwell on one.

Wireshark and its application in digital forensics were considered in this paper. The methods of its application for detecting unauthorized access to the network, infecting devices with malicious botnets, detecting connections to Tor networks, and finding peer-to-peer network nodes and others are very easy and powerful. Scenarios for using this packet analyzer are quite diverse. The open-source code and its large functionality allow it to be embedded in detection systems for different types of attacks. Nowadays, the study of network security systems using Wireshark based on machine learning is becoming more popular. Thus, the use of this powerful tool helps in the investigation of crimes. Primary response right after an incident is detected with the help of Wireshark may improve the detection of cybercrimes and reduce losses from them.

REFERENCES

1. Official site of online publications *Finmarket.ru* - Sberbank assess the loses of the world's economy after cyberattacks in 2019. – [Text: electronic] – URL: http://www.finmarket.ru/news/5154437 / (Reference date 10.12.2021).

2. Shaoqiang Wang, DongSheng Xu, ShiLiang Yan. - Analysis and Application of Wireshark in TCP/IP Protocol Teaching. // International Conference on E-Health Networking, Digital Ecosystems, and Technologies. / [Text: electronic] – 2010. – p. 269-272. (Reference date 10.12.2021).

3. Kazenas G. V. Wireshark: more advantages than disadvanteages. // Languages in professional communication. International research to practice conference for educators, postgraduates and students. / Text: electronic. – 28 May. 2020. – p. 533-537. (Reference date 10.12.2021).

4. Zoltán Balogh, Štefan Koprda, Jan Francisti. - LAN security analysis and design. // IEEE 12th International Conference on Application of Information and Communication. / Text: electronic. – October, 2018. (Reference date 10.12.2021)

5. Myint Soe Khaing, Yee Mon Thant, Thazin Tun, Chaw Su Htwe, Mie Mie Su Thwin. – IoT Botnet Detection Mechanism Based on UDP Protocol design. // 2020 IEEE Conference on Computer Applications (ICCA). / Text: electronic. – 27-28 Feb. 2020. (Reference date 10.12.2021).

6. Kotey Seth Djanie, Tchao Eric Tutu, Gadze James Dzisi. - A Proposed DoS Detection Scheme for Mitigating DoS Attack Using Data Mining Techniques. // Computers. / Text: electronic. - 26 November, 2019. (Reference date 10.12.2021)

7. Deepak Kshirsagara, Amit Rathodb, Sachin Wathoreca. - Performance analysis of DoS LAND attack detection. // Perspectives in Science. / Text: electronic. – September, 2016. (Reference date 10.12.2021).

8. Leslie F. Sikos. - Packet analysis for network forensics: A comprehensive survey. // Forensic Science International: Digital Investigation. / Text: electronic. - 1 October, 2019. (Reference date 10.12.2021).

9. Shivani Gaonkar, Ashlesha Borkar, Nandini Fal Dessai, Shailendra Aswale, Jenny Costa, Pratiksha Shetgaonkar. – A Survey on Botnet Detection Techniques. // International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE). / Text: electronic. – 2020. (Reference date 10.12.2021).

10. Lapshichyov V., Makarevich O. – TLS certificate as a sign of establishing a connection with the network Tor. // International Conference on Security of Information and Networks. / Text: electronic. – September, 2019. (Reference date 10.12.2021).

11. Ahmad Musa, Aliyu Abubakar, Usman Abdul Gimba. – An Investigation into Peer-to-Peer Network Security Using Wireshark. // International Conference on

Electronics Computer and Computation (ICECCO 2019). / Text: electronic. – 10-12 December, 2019. (Reference date 10.12.2021).

12. Felix Larbi Aryeh, Boniface Kayode Alese, Olayemi Olasehinde. – Graphical analysis of captured network packets for detection of suspicious network nodes. // International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). / Text: electronic. –15-19 June 2020. (Reference date 10.12.2021).